



WINDHAM SCHOOL
DISTRICT

NUMBER: SD-10.14
DATE: March 24, 2008
PAGE: 1 of 3
SUPERSEDES: OP-10.11
November 17, 2004

SUPERINTENDENT DIRECTIVE

SUBJECT: INFORMATION RESOURCES ACCEPTABLE USE

AUTHORITY: Windham Board Policy 3.02

APPLICABILITY: Windham School District (WSD or District)

POLICY:

Information resources shall be used to support District efforts to provide educational programming and services for eligible offenders.

DEFINITIONS:

“Access” means to interact with or otherwise make use of information resources.

“Information Resources” (IR) are any and all computer printouts, online display devices, magnetic/optical or other storage media, and all computer-related activities involving any device capable of receiving email, browsing web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, thin-client devices, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled equipment, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, they are the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

“Network” refers to all data transport networks used primarily to interconnect computers and networks of computers for the purpose of transporting data, allowing interoperation of computer applications on more than one computer system, and providing access to data.

PROCEDURES:

I. General Use and Ownership

- A. All users accessing the TDCJ Wide Area Network shall adhere to the TDCJ policies governing use of the system including, but not limited to, AD-15.07, AD-15.08, AD-15.15, and ED-15.11.
- B. Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of WSD are the property of the District.
- C. Information resource files are not private and may be accessed by authorized District Computer Services Department (CSD) employees at any time without knowledge of the information resources user or owner.
- D. WSD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- E. All messages, files and documents located on District information resources are subject to Open Records requests, and may be accessed in accordance with this policy.

II. Unacceptable Use:

Unacceptable use involves the use of District information resources for purposes other than which they were intended. Unacceptable use may include, but not be limited to:

- A. Engage in any activity that is illegal under local, state, or federal law while utilizing District owned resources.
- B. Make unauthorized copies of software without written permission of the copyright holder.
- C. Export software, technical information, encryption software or technology, in violation of international or regional export control laws. The Administrator, CSD should be consulted prior to the export of any material.
- D. Intentionally introduce malicious programs into the network (e.g., viruses, worms, Trojan horses, E-mail bombs).
- E. Attempt to access any data or programs contained on District or other systems for which the user does not have authorization or explicit consent.
- F. Intentionally access, create, store or transmit material that may be offensive, indecent, or obscene in nature.
- G. Use personally owned computer devices without the approval of Division Director or designee. These include but are not limited to computers, laptops, PDA, floppy disk, CD ROM, and USB devices.

- H. Purposely engage in activity that may:
1. Be illegal, in support of illegal activities, or be prohibited by District policies;
 2. Harass, threaten or abuse others;
 3. Degrade the performance of information resources;
 4. Deprive authorized WSD user(s) access to any District information resources;
 5. Obtain extra resources beyond those allocated;
 6. Circumvent District computer security measures;
 7. Result in personal profit or gain;
 8. Cause misuse or damage to equipment or systems;
 9. Disclose dialup or dial back modem phone numbers to unauthorized personnel;
 10. Permit port or security scanning; or
 11. Allow the download, installation, or running of security programs or utilities that reveal or exploit weaknesses in the security of a system, unless this activity is a part of the employee's normal job duty.

Debbie Roberts, Superintendent
Windham School District